

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO**

In the Matter of the Search of:)	No. 2:24-mj-292
)	
The email accounts, including all information and content, associated with the Google email addresses listed in Attachment A and collectively referred to as SUBJECT ACCOUNTS, that are stored at the Premises Controlled by Google, Inc.)	Magistrate Judge Vascura
)	
)	<u>UNDER SEAL</u>

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Amanda North (Your Affiant), a Special Agent with the Ohio Bureau of Criminal Investigation (BCI) and assigned as a Task Force Officer (TFO) for the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

EDUCATION TRAINING AND EXPERIENCE

1. I am a Special Agent (SA) with BCI, since 2022, and have been in the Special Victims Unit since 2013, where I was previously a Criminal Investigator. I have been a TFO at the FBI Columbus Resident Agency since early 2023. I am primarily responsible for investigating child sexual exploitation and internet crimes, as well as hands on offenses of abuse involving juveniles and the elderly.

2. During my career as a Criminal Investigator, I have received more than one hundred hours of training in internet investigations, to include Peer to Peer software. I was assigned full-time to the Franklin County Internet Crimes Against Children Task Force (ICAC), from January of 2016 through my promotion to SA in May of 2022. I was also a TFO for Homeland Security from 2018 until the end of 2021, when I was designated to be assigned to the FBI VCAC Unit. I have participated in various investigations of child exploitation and have executed numerous search warrants, interviews and arrests that resulted in conviction. As part of my duties as a TFO, I investigate criminal violations relating to child exploitation and child pornography violations, including the illegal production, distribution, transmission, receipt, and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A.

3. As a TFO with the FBI, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

PURPOSE OF THE AFFIDAVIT

4. I make this affidavit in support of an application for a search warrant for information associated with the following email addresses from Google email accounts:

- a. Nickolastravis92@gmail.com;
- b. Bigwiz6542@gmail.com;
- c. Buddylee6542@gmail.com;
- d. Wisdomodafi@gmail.com;
- e. odafiwisdom@gmail.com;
- f. wezykelvin@gmail.com;
- g. Wicixllc@gmail.com;
- h. andersonzehh@gmail.com;
- i. kewizzchannel@gmail.com;
- j. Jarianlorenzo@gmail.com;

(collectively the **SUBJECT ACCOUNTS**) that is stored at premises controlled by Google, a Google of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google, Inc. to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber or customer associated with the **SUBJECT ACCOUNTS**.

5. The **SUBJECT ACCOUNTS** to be searched are more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A— sexual exploitation of a minor and distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the **SUBJECT ACCOUNTS**, wherein the items specified in

Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of crime.

6. The facts set forth below are based upon my knowledge, experience, observations, and investigation, as well as the knowledge, experience, investigative reports, and information provided to me by other law enforcement agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every known fact to me relating to the investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of 18 U.S.C. §§ 2251, 2252, 2252A— sexual exploitation of a minor and distribution, transmission, receipt, and/or possession of child pornography are presently located in the **SUBJECT ACCOUNTS**. I have not omitted any facts that would negate probable cause.

APPLICABLE STATUTES AND DEFINITIONS

1. Title 18 United States Code, Section 2251(a) makes it a federal crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in, or have a minor assist any other person to engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, if such person knows or has reason to know that either the visual depiction will be transported or transmitted via a facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, or that the visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce, or if the visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce. Subsection (e) of this provision further prohibits conspiracies or attempts to engage in such acts.
2. Title 18, United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting

interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

3. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce. This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce or is in or affecting interstate commerce.

4. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

5. As it is used in 18 U.S.C. §§ 2251 and 2252, the term “sexually explicit conduct” is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

6. As it is used in 18 U.S.C. § 2252A(a)(2), the term “child pornography” is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual

depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

7. The term “sexually explicit conduct” has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), “sexually explicit conduct” also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

8. The term “minor”, as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as “any person under the age of eighteen years.”

9. The term “graphic,” as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean “that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted.”

10. The term “visual depiction,” as used herein, is defined pursuant to 18 U.S.C. § 2256(5) to “include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image.”

11. The term “computer” is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

12. The terms “records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media

Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

13. “Cellular telephone” or “cell phone” means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books”; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may include geographic information indicating where the cell phone was at particular times.

14. Internet Service Providers” (ISPs), used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

15. “Internet Protocol address” (IP address), as used herein, is a code made up of numbers separated by dots that identifies particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses can be dynamic, meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

16. As it is used throughout this affidavit and all attachments hereto, the term “storage media” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

BACKGROUND INFORMATION REGARDING GOOGLE, GMAIL, AND TECHNOLOGY

17. Google, LLC provides its subscribers internet-based accounts that allow them to send, receive, and store e-mails online. Google accounts are typically identified by a single

username, which serves as the subscriber's default e-mail address, but which can also function as a subscriber's username for other Google services, such as instant messages and remote photo or file storage.

18. Based on my training and experience, I know that Google allows subscribers to obtain accounts by registering on Google's website. During the registration process, Google asks subscribers to create a username and password, and to provide basic personal information such as a name, an alternate e-mail address for backup purposes, a phone number, and, in some cases, a means of payment. Google typically does not verify subscriber names. However, Google does verify the e-mail address or phone number provided.

19. Once a subscriber has registered an account, Google provides e-mail services that typically include folders such as an "inbox" and a "sent mail" folder, as well as electronic address books or contact lists, and all of those folders are linked to the subscriber's username. Google subscribers can also use that same username or account in connection with other services provided by Google.

20. Notably, Google, LLC also provides "cloud" storage services. Account holder/users can utilize this service, which is called "Google Drive," to store pictures, videos, and other electronic files remotely and without taking up memory space on their personal computer, smart phone, and physical storage media.

21. In general, user-generated content (such as e-mail) that is written using, stored on, sent from, or sent to a Google account can be permanently stored in connection with that account, unless the subscriber deletes the material. For example, if the subscriber does not delete an e-mail, the e-mail can remain on Google servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to exist on Google's servers for a certain period of time.

22. These services may include electronic communication services such as Google Voice (voice calls, voicemail, and SMS text messaging), Hangouts (instant messaging and video chats), Google+ (social networking), Google Groups (group discussions), Google Photos (photo sharing), and YouTube (video sharing); web browsing and search tools such as Google Search (internet searches), Web History (bookmarks and recorded browsing history), and Google Chrome (web browser); online productivity tools such as Google Calendar, Google Contacts, Google Docs (word processing), Google Keep (storing text), Google Drive (cloud storage), Google Maps (maps with driving directions and local business search) and other location services, and Language Tools

(text translation); online tracking and advertising tools such as Google Analytics (tracking and reporting on website traffic) and Google AdWords (user targeting based on search queries); Pixel Phone (services which support a Google smartphone); and Google Play (which allow users to purchase and download digital content, e.g., applications).

23. Thus, a subscriber's Google account can be used not only for e-mail but also for other types of electronic communication, including instant messaging and photo and video sharing; voice calls, video chats, SMS text messaging; and social networking. Depending on user settings, user-generated content derived from many of these services is normally stored on Google's servers until deleted by the subscriber. Similar to e-mails, such user-generated content can remain on Google's servers indefinitely if not deleted by the subscriber, and even after being deleted, it may continue to be available on Google's servers for a certain period of time. Furthermore, a Google subscriber can store contacts, calendar data, images, videos, notes, documents, bookmarks, web searches, browsing history, and various other types of information on Google's servers.

24. Based on my training and experience, I know that evidence of who controlled, used, and/or created a Google account may be found within such computer files and other information created or stored by the Google subscriber. Based on my training and experience, I know that the types of data discussed above can include records and communications that constitute evidence of criminal activity.

25. Based on my training and experience, I know that providers such as Google also collect and maintain information about their subscribers, including information about their use of Google services. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. Providers such as Google also commonly have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with other logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which devices were used to access the relevant account. Also, providers such as Google typically collect and maintain location data related to subscriber's use of Google services, including data derived from IP addresses and/or Global Positioning System ("GPS") data.

26. Based on my training and experience, I know that providers such as Google also collect information relating to the devices used to access a subscriber's account – such as laptop or desktop computers, cell phones, and tablet computers. Such devices can be identified in various ways. For example, some identifiers are assigned to a device by the manufacturer and relate to the specific machine or “hardware,” some identifiers are assigned by a telephone carrier concerning a particular user account for cellular data or voice services, and some identifiers are actually assigned by Google in order to track what devices are using Google's accounts and services. Examples of these identifiers include unique application number, hardware model, operating system version, Global Unique Identifier (“GUID”), device serial number, mobile network information, telephone number, Media Access Control (“MAC”) address, and International Mobile Equipment Identity (“IMEI”).

27. Based on my training and experience, I know that such identifiers may constitute evidence of the crimes under investigation because they can be used (a) to find other Google accounts created or accessed by the same device and likely belonging to the same user, (b) to find other types of accounts linked to the same device and user, and (c) to determine whether a particular device recovered during course of the investigation was used to access the Google account.

28. In addition, I know that Google maintains records that can link different Google accounts to one another, by virtue of common identifiers, such as common e-mail addresses, common telephone numbers, common device identifiers, common 7 computer cookies, and common names or addresses, that can show a single person, or single group of persons, used multiple Google accounts. Based on my training and experience, I also know that evidence concerning the identity of such linked accounts can be useful evidence in identifying the person or persons who have used a particular Google account.

29. Based on my training and experience, I know that subscribers can communicate directly with Google about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Providers such as Google typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the

crimes under investigation because the information can be used to identify the account's user or users.

30. In summary, based on my training and experience in this context, I believe that the servers of Google are likely to contain user-generated content such as stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers), as well as Google-generated information about its subscribers and their use of Google services and other online services. In my training and experience, all of that information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. In fact, even if subscribers provide Google with false information about their identities, that false information often nevertheless provides clues to their identities, locations, or illicit activities.

31. As explained above, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of the offense, or, alternatively, to exclude the innocent from further suspicion. From my training and experience, I know that the information stored in connection with a Google account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, e-mail communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by Google can show how and when the account was accessed or used. For example, providers such as Google typically log the IP addresses from which users access the account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the Google account access and use relating to the criminal activity under investigation. This geographic and timeline information may tend to either inculcate or exculpate the person who controlled, used, and/or created the account. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via e-mail). Finally, stored electronic data may provide relevant insight into the user's state of mind as it relates to the offense under investigation. For example, information in the Google account may indicate its user's motive and intent to

commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INVESTIGATION AND PROBABLE CAUSE

32. On or about November 23, 2023, a lead was forwarded from the FBI Washington Field Office to the FBI Columbus Office after a potential target involving the sexual exploitation of a minor was identified. The lead stemmed from an investigation out of Virginia in which a Dropbox user was uploading child pornography images in July of 2023. The upload of three images was then reported by Dropbox to the National Center for Missing and Exploited Children (NCMEC). The NCMEC, pursuant to some initial legal process related to the Dropbox user and IP information, was able to ascertain the likely target resided in Virginia and the lead was assigned to the Fairfax County Police Department (FCPD) in Fairfax, Virginia accordingly.

33. The user of the Dropbox account was identified as a Juvenile Target (JT), and on September 26, 2023, the Fairfax County Police Department interviewed JT in the presence of his/her parents. JT advised that he/she owned the Dropbox account and associated email accounts related to the upload of child pornography. Law enforcement obtained consent from the parents/guardians of JT to further search the contents of JT's cellular phone and a Telegram account associated to JT.

34. A review of the cellular device belonging to JT revealed dozens of instances in which JT distributed Mega links containing child pornography on various social media platforms. JT further attempted to purchase child pornography from other individuals online utilizing the same social media applications JT was utilizing as well.

35. One of the individuals JT communicated with was later identified as John Doe¹. In communications recovered between the two of them, JT inquired about purchasing child pornography from John Doe. In response, John Doe advised that he was selling Mega links containing various types of child pornography, and that he accepted payment for the child pornography links via PayPal, CashApp, Zelle and cryptocurrencies. John Doe provided his cashtag as \$Nickolastravis.

¹ The full name of John Doe is known to investigators but has been redacted from this affidavit to protect his identity because, as further outlined below, the investigation thus far has revealed him to be a victim of identity theft and not involved with violations of federal law related to child exploitation.

36. Legal process to CashApp for the \$Nickolastravis username revealed that the Cashapp account was owned by an individual identified as John Doe, as noted above, DOB 04/XX/1992. The address listed for John Doe noted as a residence in Byhalia, Mississippi 38611.

37. An undercover officer (OCE) further communicated with John Doe on Telegram, where John Doe distributed to the OCE a screenshot of available child pornography and a menu of options and advertisements for the sale of child pornography, as well as a video. The video appeared to be a compilation which depicted the following: a prepubescent female who was nude and performing oral sex on an adult male and a prepubescent female nude from the waist down, with her legs spread and her genitalia exposed to the camera while sitting on an adult male's lap who is simultaneously using his hand to massage the prepubescent females vagina.

38. After learning that John Doe resided in Mississippi based on the above information, the lead was sent to the FBI Jackson (Mississippi) Field Office. In further attempting to confirm the location of John Doe, law enforcement learned that John Doe was now residing in Ohio and sent to the FBI in Columbus.

39. More specifically, Ohio Law Enforcement Gateway (OHLEG) searches listed John Doe as a resident at an address in Reynoldsburg, Ohio 43068. Further research revealed John Doe resided there with his mother.

40. In further searches of law enforcement database, law enforcement learned that in October 2023, Reynoldsburg, Ohio police personnel had done an investigative check on John Doe. Agents with the FBI made contact with the Reynoldsburg Police Department (RPD) and learned that RPD had received a request from the Dallas Internet Crimes Against Children (ICAC) Task Force regarding John Doe. Per the Dallas ICAC, John Doe was under investigation after he had been identified by the ICAC as an individual advertising the sale of child pornography on Reddit.

41. On December 21, 2023, FBI agents in Columbus obtained the investigative file from the OCE who had communicated with John Doe. The file included the Telegram communications, screen shots of the child pornography sent by John Doe, and responsive data from CashApp related to the communications. That response from CashApp listed a physical address for John Doe in Reynoldsburg, Ohio. The return also listed a subscriber email address of NickolasTravis92@gmail.com.

42. Additionally, law enforcement was able to locate the account John Doe utilized on Telegram, "Big Nick ceepee". Periodic checks of the John Doe Telegram account has shown that the account has been active as recently as February 13, 2024 at 1422 hours.

43. On or about March 11, 2024, a federal search warrant for the residence of John Doe was obtained authorizing the search for and seizure of digital media devices from John Doe's residence in Reynoldsburg, Ohio. On or about March 13, 2024, that search warrant was executed, and multiple devices were seized and forensically analyzed pursuant to that warrant. Review of the devices by the FBI resulted in the determination that although John Doe's identifiers were used in the creation of the **SUBJECT ACCOUNTS**, John Doe was not the target. For example, the target email address of nickolastravis92@gmail.com was not identified in any of the forensics on John Doe's devices and it therefore appeared that an unknown individual (hereinafter UIN) had been utilizing John Doe's information.

44. The investigation also revealed that on October 19, 2023, the Dallas ICAC had submitted a search warrant to Google, LLC for content related to the nickolastravis92@gmail.com account and the results were provided to investigators for further analysis. The return results indicated that the user of that account was engaged in crypto currency exchange, which was identified in a series of emails in the inbox, specifically Coinbase and Binance, which your affiant knows to be used as cryptocurrency exchange platforms.

45. A subpoena was submitted to Coinbase for subscriber information provided a driver's license used to open the account. That drivers license included all of John Doe's identifiers, but the picture was of a male black and your affiant knows John Doe to be a male white.

46. A subpoena was also issued to Binance for subscriber information identified two user profiles: Wisdom Odafi of Nigeria and Nassim Achbo of the Netherlands. The photo of Wisdom Odafi matched the image on the John Doe fraudulent drivers license noted above.

47. Further review of the Google Subscriber information for the nickolastravis92@gmail.com account responsive data provided a recovery email listed as buddylee6542@gmail.com.

48. In the search warrant return, Google also provided a list of four different devices that had been utilized to log into the nickolastravis92@gmail.com account. In addition, Google noted other email addresses that had utilized those same four devices which your affiant knows to mean that the following accounts were accessed on the same devices nickolastravis92@gmail.com

email account was and most likely by the same user: wisdomodafi@gmail.com,
wezykelvin@gmail.com; odafiwisdom@gmail.com; wicixllc@gmail.com;
andersonzehh@gmail.com; bigwiz6542@gmail.com; kewizzchannel@gmail.com;
jarianlorenzo@gmail.com.

49. Also recovered from the Nickolastravis92@gmail.com account returns was an email that the user sent to another individual which stated, in summary, that when selling child pornography, the UIN did not use his real identity and utilized a numerous of different identities. Based on the investigation thus far in conjunction with the statements made by the UIN and your affiants training and experience, the **SUBJECT ACCOUNTS** that were identified through the nickolastravis92@gmail.com responsive data indicated that the UIN is utilizing multiple email addresses and accounts, including that of John Doe, in an effort to conceal their identity and evade law enforcement detection. Those accounts, identified above, are believed to contain information and evidence that will further aid law enforcement with the identification of those responsible for selling, distributing, and possessing child pornography via creating fake identities or stealing the identities of others.

**COMMON CHARACTERISTICS OF INDIVIDUALS WITH A
SEXUAL INTEREST IN CHILDREN**

50. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children.

- a. Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.
- b. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media,

including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

- c. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.
- d. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.
- e. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and videos have been deleted from the computers or digital media.

51. Based upon the conduct of individuals involved in seeking/soliciting, receiving, distributing, and/or collecting child pornography set forth in the above paragraphs, and the facts learned during the investigation in this case, namely, that an individual utilizing the identity of John Doe as a means to conceal their true identity, was engaged in the sale of child pornography on various platforms, communicating with likeminded individuals who were sharing images and videos of child pornography. The unknown user engaged in conversations in Telegram and on Reddit, where he advertised for sale links to Mega containing child pornography images, indicating his interest in the sexual exploitation of juveniles, and therefore, your affiant has reason to believe that this user has a sexual interest in minors and has viewed or sought out visual depictions of minors engaged in sexually explicit conduct utilizing an internet-capable device. Your affiant therefore submits that there is probable cause to believe the evidence of violations of 18 U.S.C. §§ 2251, 2252, 2252A– sexual exploitation of a minor and distribution, transmission, receipt, and/or possession of child pornography will be located in the **SUBJECT ACCOUNTS**.

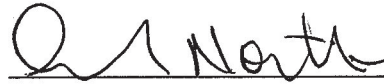
INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

52. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment.

CONCLUSION

53. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of 18 U.S.C. §§ 2251, 2252, 2252A– sexual exploitation of a minor and distribution, transmission, receipt, and/or possession of child pornography have been committed, and evidence of those violations is located on the person described in **Attachment A** and in the residence described in Attachment B. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in **Attachment B**.

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Furthermore, because the warrant will be served on Google, LLC, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.



Amanda North
TFO

Federal Bureau of Investigation

Sworn to and subscribed before me this 3rd day of June, 2024.



~~XXXXXXXXXXXXXXXXXXXX~~ Elizabeth A. Preston Deavers Chelsey M Vascara
United States Magistrate Judge
United States District Court
Southern District of Ohio